Matematiikan laitos
Teknillinen korkeakoulu Turunen/Masson

Mat-1.3111 Lukuteoria

Tentti 7.3.2007

Täytä selvästi *jokaiseen vastauspaperiin* kaikki otsaketiedot. Merkitse kuulustelukoodi-kohtaan opintojakson numero, nimi ja onko kyseessä tentti vai välikoe. $\star$-kohta jätetään tyhjäksi. Koulutusohjelmakoodit ovat ARK, AUT, EST, INF, KEM, KON, MAA, MAK, MAR, PUU, RYK, TFY, TIK, TLT, TUO.

Kokeessa saa käyttää funktiolaskinta, ei muita apuvälineitä. Koeaika on 3 tuntia.

1. Laske Eukleideen algoritmilla $\gcd(520, 413)$. Etsi yhtälön

$$520x \equiv 1 \pmod{413}$$

ratkaisut.

2. Muotoile ja todista kiinalainen jäännöslause yhtälöryhmälle

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}. \end{cases}$$

3. Määrittele Eulerin φ -funktio. Etsi alkuluvut p ja q, joista tiedetään että

$$\begin{aligned} pq &= 2866769, \\ \varphi(pq) &= 2863344. \end{aligned}$$

4. Lasketaan $\left(\frac{2}{p}\right)$, kun $p \neq 2, p \in \mathbb{P}$. Täydennä ja perustele yksityiskohtaisesti seuraavan päättelyn kaikki toteamukset ja välivaiheet:

Määritellään

$$\alpha := \mathrm{e}^{\mathrm{i}2\pi/8},\ x := \alpha + \bar{\alpha}.$$

Pätee

$$x^2 = 2.$$

$\Longrightarrow$

$$\left(\frac{2}{p}\right) \equiv x^{p-1} \pmod{p}.$$

Toisaalta pätee

$$x^p \equiv \alpha^p + \bar{\alpha}^p \pmod{p\mathbb{Z}[\alpha]},$$

ja

$$\alpha^p + \bar{\alpha}^p = (-1)^{\frac{p^2-1}{8}} x.$$

$\Longrightarrow$

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p\mathbb{Z}[\alpha]}.$$

$\Longrightarrow$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$